Implementing security.txt

# Implementing security.txt

Domains where the Ministry of Justice (MoJ) is primarily responsible for cyber security **must** redirect the /.well-known/security.txt location to the central security.txt file.

This redirection should be accessible from the public Internet whether or not the underlying applications/systems are. For example, https://test.not-production.justice.gov.uk may be a web-application requiring authentication, however https://test.not-production.justice.gov.uk/.well-known/security.txt should still be accessible without authentication.

## security.txt

/.well-known/security.txt must HTTP 301 (permanent redirect) to https://raw.githubusercontent.com/ministryofjustice/security-guidance/main/contact/vulnerability-disclosure-security.txt.

For example, https://www.prisonvisits.service.gov.uk/.well-known/security.txt must HTTP 301 to https://raw.githubusercontent.com/ministryofjustice/security-guidance/main/contact/vulnerability-disclosure-security.txt.

### /.well-known/

We use /.well-known/ to house security.txt as [RFC5785](https://tools.ietf.org/html/rfc5785) defines it as a path prefix for "well-known locations" in selected Uniform Resource Identifier (URI) schemes.

## Internal-facing domains

Internal-facing domains resolvable from the public Internet (for example, intranet.justice.gov.uk is based on .gov.uk with a publicly routeable IP address) should also implement security.txt as described above.

## Non-production domains

Non-production domains resolvable from the public Internet (for example, a demo deployment of a MoJ digital service or prototype) should also implement security.txt as described above.